WHAT IS CLAIMED IS:

1. A method of reducing denial-of-service attacks by malicious mobile nodes in a mobile IP environment, said method comprising:

maintaining, by each of a plurality of access routers within the mobile IP environment, a cache of neighboring access routers as candidates and their associated access points; and

populating the caches with cache entries in response to actions initiated by mobile nodes, wherein

each cache entry is tagged with an identity of an action initiating mobile node, which identity is based on information that is verifiable by the access routers and which cannot be modified arbitrarily by the mobile node, and

wherein a total number of entries that can be tagged and thus introduced into a cache by any given node is limited.

2. A method of validating information of a mobile node within a candidate access router discovery procedure in a mobile IP environment, said method comprising:

generating a token by a first access router to which the mobile node was previously attached;

sending the token from the first access router to the mobile node within a message comprising a list of candidate access routers;

sending the token from the mobile node to a second access router as selected candidate after a handover procedure between the first and second access routers;

sending the token within an exchange between the access routers specific to the discovery procedure from the second access router back to the first access router for verification.

3. The method according to claim 1, wherein the identity of the mobile node is an international mobile subscriber identity (IMSI) for cellular

communication systems, and a network access identifier (NAI) for systems based on Internet Protocol (IP).

4. The method according to claim 1, wherein an action initiated by a mobile node comprises a handover procedure of the mobile node between a previous access router and a new access router, said method further comprising:

generating a token by the previous first access router;

sending the token from the previous access router to the mobile node within a message comprising a list of candidate access routers;

sending the token within a message specific to the discovery procedure from the mobile node to the new access router as selected candidate after the handover procedure;

sending the token within a neighbor exchange between the access routers resulting in cache entries being created or refreshed from the second access router back to the first access router for verification.

5. The method according to claim 4, wherein

the token is generated by maintaining by the previous access router a short list of random values used as keys to hash the identity of the mobile node,

each key in the short list is associated with an integer index that is passed along with the token, and wherein

upon receiving the token for verification, the previous access router uses the integer index to lookup the associated key, hash the identity of the mobile node sent in the neighbor exchange and compares the hash to the token.

6. The method according to claim 5, wherein with progressing time new keys are generated and added to the head of the list while old keys are expired and removed so that from the length of the list and the frequency of generated keys, the total amount of time is determined a mobile has been attached.

7. A system for reducing denial-of-service attacks by malicious mobile nodes in a mobile IP environment, said system comprising:

a plurality of access routers within the mobile IP environment, each router maintaining a cache of neighboring access routers as candidates and their associated access points; and

a plurality of mobile nodes which are capable of populating the caches in response to actions initiated, wherein

the cache is configured such that each cache entry is tagged with an identity of the action initiating mobile node having thus created the entry, and that a total number of entries that can be tagged and thus introduced into the cache by any given node is limited.

8. A system for validating information of a mobile node within a candidate access router discovery procedure in a mobile IP environment, comprising a first access router, said mobile node and a second access router, wherein:

the first access router includes generating means for generating a token, first sending means for sending the token to the mobile node within a message comprising a list of candidate access routers,

the mobile node includes second sending means for sending the token to the second access router as selected candidate after a handover procedure between the access routers, and wherein

the second access router includes third sending means for sending the token within an exchange between the access routers specific to the discovery procedure back to the first access router and verification means for verifying the token.

9. The system according to claim 7, wherein

the access routers include generating means for generating a token, first sending means for sending the token to a mobile node within a message comprising a list of candidate access routers, second sending means for sending

the token within a neighbor exchange between access routers resulting in cache entries being created or refreshed, and verification means for verifying the token; and wherein

the mobile nodes include third sending means for sending the token to a new access router as selected candidate after a handover procedure.

10. The system according to claim 9, wherein

the generating means include first hashing means for hashing the identity of the mobile node by using random values out of a short list as keys, associating means for associating each key in the list with an integer index, and wherein

the verification means include a lookup table for the indices and their associated keys, second hashing means for hashing the identity of the mobile node and comparing means for comparing the hash to the token.

11. The system according to claim 10, wherein

the generating means are configured to generate new keys with progressing time, to add them to the head of the list, and to remove old keys; the system further comprising

determination means for determining a total amount of time a mobile has been attached from the length of the list and the frequency of generated keys.

12. An access router for reducing denial-of-service attacks by malicious mobile nodes in a mobile IP, said router comprising:

a cache of neighboring access routers as candidates and their associated access points, wherein

the cache is arranged such that each cache entry is tagged with the identity of the mobile node having initiated the entry creation, and that the total number of entries that can be tagged and thus introduced into the cache by any given node is limited.

13. An access router for validating information of a mobile node in a mobile IP, comprising:

generating means for generating a token;

first sending means for sending the token to the mobile node within a message comprising a list of candidate access routers;

second sending means for sending the token within an exchange with another access router specific to the discovery procedure to the other access router; and

verification means for verifying the token.

14. The access router according to claim 12, further comprising:

generating means for generating a token,

first sending means for sending the token to a mobile node within a message comprising a list of candidate access routers,

second sending means for sending the token within a neighbor exchange with another access router resulting in cache entries being created or refreshed, and

verification means for verifying the token.

15. The access router according to claim 14, wherein

the generating means include first hashing means for hashing the identity of the mobile node by using random values out of a short list as keys, associating means for associating each key in the list with an integer index, and

the verification means include a lookup table for the indices and their associated keys, second hashing means for hashing the identity of the mobile node and comparing means for comparing the hash to the token.

16. The access router according to claim 15, wherein

the generating means are configured to generate new keys with progressing time, to add them to the head of the list, and to remove old keys.